PS-08-004 Computer Security Incident Management
Issue Date: 3/20/2008
Revision Effective Date: 3/20/2008
Review Date: 12/1/2020

PURPOSE
The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Through implementing solid security policies, limiting access to networks and computers, improving user security awareness, and early detection and mitigation of security risks are some the preventative actions that can be taken to reduce the risk, frequency and the cost of security incidents, not all incidents can be prevented. Therefore an incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

This policy establishes the requirement for each agency to establish an internal capability for handling computer security incidents.

POLICY
Each agency shall establish and document an internal security incident management capability that provides for prevention, monitoring, detection, containment, response, recovery, reporting and escalation appropriate to the level of risk and threats to the organization.

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES
Incident Response and Reporting (SS-08-004)

REFERENCES
NIST Document 800-61, Computer Security Incident Handling Guide
https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

TERMS and DEFINITIONS
Incident Management is the process of detecting, mitigating, and analyzing threats or violations of security policies and controls and limiting their effect.

Computer Security Incident is a violation (breach) or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices which may include, but are not limited to: widespread infections from virus, worms, Trojan horse or other malicious code; unauthorized use of computer accounts and computer systems; unauthorized, intentional or inadvertent disclosure or modification of sensitive/critical data or infrastructure; intentional disruption of critical system functionality; intentional or inadvertent penetration of firewall; compromise of any server, including Web server defacement; exploitation of other weaknesses; child pornography; attempts to obtain information to commit fraud or otherwise prevent critical operations or cause danger to state or national security; and violations of the State security policies or standards that threaten or compromise the security objectives of the State's data, technology or communications systems.